STATE of ARIZONA

Government Information Technology Agency	**Statewide STANDARD** P740-S741	**TITLE: Classification and Categorization of Data** Effective Date: August 15, 2003

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))), including, the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

The purpose of this standard is to identify baseline classifications for data/information for which the State is considered the owner[1,2]. It is intended to establish a data classification methodology to selectively protect data/information in the State's custody against loss or misuse.

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSP) within each Budget unit.

4. STANDARD

This standard establishes that data/information shall be classified according to its degree of sensitivity in a universally understandable manner, and that such data/information shall maintain its security classification as it traverses any physical or logical boundary such as a budget unit, computer-related device, network, or software application system.

---

[1] Unless otherwise defined by statute or federal mandates and regulations, the Budget Unit CEO is considered the owner of data/information within the authority of a budget unit, and may delegate ownership responsibilities as specified herein. Ownership assignment and responsibility considerations include which budget unit collects the data/information; is responsible for the accuracy and integrity of the data/information; incurs the cost associated with gathering, managing, and storing the data/information; and is most affected by the loss of confidentiality, integrity, and availability of the data/information.

[2] Owners of data/information are responsible for establishing the rules for appropriate use and protection of the subject data/information (rules of behavior). The data/information owner retains that responsibility even when the data/information is shared with other organizations. [Source: NIST SP 800-18].

4.1. DATA/INFORMATION SHALL BE DIVIDED INTO THE FOLLOWING CLASSIFICATIONS.

- **Confidential Data/Information**: data whose loss, corruption, or unauthorized disclosure would be a violation of Arizona Revised Statues or federal mandates and regulations. Confidential is understood to be a continuum wherein some data/information is more sensitive than other data/information and shall be protected in a more secure manner.
- **Public Information**: data that is made generally available without specific custodian approval and that has not been explicitly and authoritatively classified as confidential.

4.2. Budget units requiring additional classifications may create and document those classifications and related owner/custodian/recipient responsibilities at their discretion; however, budget units shall not impose additional classification requirements and responsibilities beyond their statutory authority and obligations.

4.3. Budget units should identify and segregate confidential data/information from public data/information either by file structure, specific accessibility, and/or presentation to prevent confidential data/information from being made directly accessible to the public.

4.4. Data/information, regardless of medium and/or form, shall be:

4.4.1. Classified as either Confidential or Public and consistently documented in a repository (i.e., database, spreadsheet, table, list document, etc.). Data/Information shall be classified as Public, unless otherwise specified by the owner.

4.4.2. Accessed in accordance with *Statewide Policy P800, IT Security; Statewide Standard P800-S810, Account Management; Statewide Standard P800-S820, Authentication and Directory Services*; and *Statewide Standard P800-S850, Encryption Technologies*.

4.4.3. Used in a manner commensurate with its classification and in accordance with applicable statutes.

4.4.4. Disposed of in accordance with applicable standards, *Records Retention and Disposition for Arizona State Agencies*, and *Arizona Electronic Recordkeeping Systems (ERS) Guidelines*, pursuant to A. R. S. § 41-1346 (8) and § A. R. S. 41-1351, as well as *Statewide Standard P800-S880, Media Sanitizing/Disposal*.

4.4.5. Made secure in accordance with *Statewide Policy P800, IT Security*, against unauthorized creation, updating, processing, outputting, and distribution.

4.4.6. Controlled relative to *Statewide Policy P800, IT Security; Statewide Standard P800-S810, Account Management; Statewide Standard P800-S820, Authentication and Directory Services; Statewide Standard P800-S825, Session Controls; Statewide Standard P800-S850, Encryption Technologies*; confidentiality requirements; Federal

and State budget unit privacy policies; *Statewide Policy P170, Privacy*; as well as applicable statutes to ensure public trust, exert the proper stewardship over, and help ensure the integrity of the data/information.

4.5. Aggregates of data/information shall be classified as to the most secure classification level of any individual component. Extracts of data/information shall be secured to the same level as the file/database from which the data/information has been extracted.

4.6. Data/information being shared with other budget units, government entities, and the private sector shall be appropriately and consistently classified based on its original classification, and protected comparable to the protection provided when the data/information is within the original budget unit's immediate control. Budget units, prior to disseminating or sharing data/information, are responsible for communicating the value and classification of the data/information to the respective additional custodians/recipients.

4.7. Classification of data responsibilities include:

4.7.1. Owners of data/information electing to delegate ownership responsibilities shall provide written delegated authority and/or signature approval for ownership responsibilities as well as specific security access permissions for database/security administrators, or those who carry out such responsibilities.

4.7.2. Owners, or those delegated their authority, shall as appropriate, assign the Confidential classification to data/information at the time the data/information is created[3] and communicate the Confidential classification to custodians, recipients, and database/security administrators, or those who carry out such responsibilities.

4.7.3. Custodians and recipients of data/information are responsible for knowing and complying with security measures applicable to the classification assigned by the owner, for informing the owner if full compliance cannot be achieved, and in accordance with *Statewide Standard P800-S855, Incident Response and Reporting*, of any compromise or possible compromise of confidential information.

4.7.4. Database/Security administrators, or those who carry out such responsibilities, upon receiving delegated authority and/or signature approval for ownership responsibilities as well as specific security access permissions, shall provide access to confidential data/information in accordance with *Statewide Standard P800-S810, Account Management*, and are responsible for ensuring that the rules

[3] Data/information is considered to be created when a software application system or a database is designed and established prior to conventional availability and use. Optimally, Confidential data/information classifications are designated during the software development cycle prior to actual data/information being entered and accessed.

for confidential information are known and followed by custodians and recipients by:

- Maintaining accurate records to ensure a full audit trail.
- Educating custodians and recipients relative to confidential data/information procedures.
- Ensuring that adequate physical protection is applied.
- Reviewing compliance periodically and reporting findings to the owners of the data/information.
- Conducting or providing oversight for audits.
- Escalating identified areas of non-compliance to the owners of the data/information.

4.8. CATEGORIZE AND PROTECT DATA/INFORMATION, AND SOFTWARE APPLICATION SYSTEMS IN ACCORDANCE WITH RISK.

The State's security objectives for data/information, and the software application systems that collect, manage, and process data/information are to protect confidentiality and preserve integrity while allowing the appropriate availability. The existence of a variety of threats, both intentional and unintentional, acting to compromise the security of data/information, as well as software application systems is recognized. In accordance with *Statewide Policy P800, IT Security*, risk levels are more heavily weighted toward the impact of the loss of confidentiality, integrity, and availability on budget unit operations, budget unit assets, or individuals than on the threat of loss.

4.8.1. Levels of risk are:

1. **Low** if the event could be expected to have a limited adverse effect on budget unit operations[4], assets, or individuals.[5] The event could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.
2. **Moderate** if the event could be expected to have a serious adverse effect on budget unit operations, assets, or individuals. The event could be expected to cause significant degradation in mission capability, place the budget unit at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.
3. **High** if the event could be expected to have a severe or catastrophic adverse effect on budget unit operations, assets, or individuals. The event could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

[4] Budget unit operations include mission, functions, image, and reputation.
[5] Adverse effects on individuals may include, but are not limited to, harm to the privacy to which individuals are entitled under law.

Categorization of data/information and software application systems includes risk levels of confidentiality, integrity and availability. The following table summarizes the security objectives and their risk levels.

	Level of Risk		
Security Objective	**Low**	**Moderate**	**High**
Confidentiality			
1. The unauthorized disclosure of data/information could be expected to have:	a limited adverse effect on budget unit operations, budget unit assets, or individuals.	have a serious adverse effect on budget unit operations, budget unit assets, or individuals.	a severe or catastrophic adverse effect on budget unit operations, budget unit assets, or individuals.
2. A loss of confidentiality could be expected to cause:	a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	significant degradation in mission capability, places the budget unit at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.
Integrity			
1. The unauthorized modification or destruction of data/information could be expected to have:	a limited adverse effect on budget unit operations, budget unit assets, or individuals.	have a serious adverse effect on budget unit operations, budget unit assets, or individuals.	a severe or catastrophic adverse effect on budget unit operations, budget unit assets, or individuals.
2. A loss of integrity could be expected to cause:	a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	significant degradation in mission capability, places the budget unit at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.
Availability			
1. The unauthorized disruption of access to or the use of data/information could be expected to have:	a limited adverse effect on budget unit operations, budget unit assets, or individuals.	have a serious adverse effect on budget unit operations, budget unit assets, or individuals.	a severe or catastrophic adverse effect on budget unit operations, budget unit assets, or individuals.
2. A loss of availability could be expected to cause:	a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	significant degradation in mission capability, places the budget unit at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

Source: FIPS PUB 199, Categorization of Information and Information Systems

The standardized format for documenting security categories is as follows:

CATEGORIZATION = [(confidentiality, RISK-LEVEL**), (integrity,** RISK-LEVEL**), (availability,** RISK-LEVEL**)**

4.8.2. Software application systems may contain multiple types of information, each of which is subject to security categorization. The determination of security categorization for a software application

system that gathers, manages, and processes multiple types of data/information shall be based on the highest level of risk determined for each type of data/information within the security categorizations of confidentiality, integrity, and availability, taking into account dependencies among these objectives.

4.8.3. Security categorizations should be used in conjunction with the development and implementation of system and environment security plans and risk assessments, as specified in *Statewide Standard P800-S805, Risk Management.*

5. DEFINITIONS AND ABBREVIATIONS

5.1. **Availability** is ensuring timely and reliable access to and use of information. The loss of availability is the disruption of access to or use of information or an information system. [44 U.S.C., Sec. 3542]

5.2. **Confidentiality** is preserving authorized restrictions of information access and disclosure, including means for protecting privacy and proprietary information. The loss of confidentiality is the unauthorized disclosure of information. [44 U.S.C., Sec. 3542]

5.3. **Integrity** is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The loss of integrity is the unauthorized modification or destruction of information. [44 U.S.C., Sec. 3542]

5.4. Refer to the Glossary of Terms located on the GITA website at http://www.gita.state.az.us/policies_standards for additional definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."

6.2. A. R. S. § 41-1335 ((A (6 & 7))), "State Agency Information."

6.3. A. R. S. § 41-1339 (A), "Depository of State Archives."

6.4. A. R. S. § 41-1346 (8), "State and local public records management; violation; classification; definition."

6.5. A. R. S. § 41-1351, "Determination of value; disposition."

6.6. A. R. S. § 41-1461, "Definitions."

6.7. A. R. S. § 41-1463, "Discrimination; unlawful practices; definition".

6.8. A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."

6.9. A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."

6.10. A. R. S. § 41-3501, "Definitions."

6.11. A. R. S. § 41-3504, "Powers and Duties of the Agency."

6.12. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."

6.13. A. R. S. § 44-7041, "Governmental Electronic Records."

6.14. Arizona Administrative Code, Title 2, Chapter 7, "Department of Administration Finance Division, Purchasing Office."

6.15. Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."
6.16. Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."
6.17. Arizona State Library, Archives and Public Records, "Arizona Electronic Recordkeeping Systems (ERS) Guidelines."
6.18. Arizona State Library, Archives and Public Records, "Records Retention and Disposition for Arizona State Agencies."
6.19. Federal Information Processing Standards Publication (FIPS PUB) 199, "Standards for Security Categorization of Federal Information and Information Systems."
6.20. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, "Guide for Development of Security Plans for Information Technology Systems."
6.21. Office of Management and Budget (OMB) Circular No. A-130, Revised (Transmittal Memorandum No. 4), "Management of Federal Information Resources."
6.22. State of Arizona Target Data/Information Architecture.
6.23. Statewide Policy P100, Information Technology.
6.24. Statewide Policy P700, Enterprise Architecture.
6.25. Statewide Policy P740, Data/Information Architecture.
6.26. Statewide Policy P800, IT Security.
- 6.26.1 Statewide Standard P800-S805, Risk Management.
- 6.26.2 Statewide Standard P800-S810, Account Management.
- 6.26.3 Statewide Standard P800-S820, Authentication and Directory Services.
- 6.26.4 Statewide Standard P800-S825, Session Controls.
- 6.26.5 Statewide Standard P800-S850, Encryption Technologies.
- 6.26.6 Statewide Standard P800-S855, Incident Response and Reporting.

6.27. United State Code Title 44, Section 3542, "Federal Information Management Act of 2002 (FISMA)," Definitions.

7. ATTACHMENTS

None.